ARKANSAS SUPREME COURT

OFFICE OF THE REPORTER OF DECISIONS
625 MARSHALL ST., SUITE 1400
LITTLE ROCK, ARKANSAS 722201

REQUEST FOR PROPOSALS

HARDWARE, SOFTWARE, AND INTEGRATION SERVICES FOR ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS FOR THE PUBLICATION OF THE OPINIONS OF THE ARKANSAS SUPREME COURT AND ARKANSAS COURT OF APPEALS

DATE: April 1, 2009

TABLE OF CONTENTS

SECTION 1
Introduction and Overview

SECTION 2

SECTION 3
Specifications

SECTION 4

SECTION 5
Proposal Submittal Documents

SECTION 1
INTRODUCTION AND OVERVIEW

1.1 Introduction

The office of the Reporter of Decisions for the Arkansas Supreme Court and Arkansas Court of Appeals (ROD) invites proposals for systems and services for implementation of a comprehensive Electronic Document Management System (EDMS) for electronic publication of the opinions of the Arkansas Supreme Court and Arkansas Court of Appeals. This system will be utilized by the ROD and must be capable of imaging both paper and electronic documents, storing them on CD-ROMS or other optical storage media for archiving and disaster recovery, and making them accessible via the Arkansas Judiciary's existing network and over the Internet. This project will require a scalable software license that can be increased as the scope of project expands.

1.2 Vendor Conference

No vendor conference will be held.

1.3 Proposed Schedule

	Activity	**Date**
a.	Request for Proposals (RFP) Published	April 1, 2009
b.	Proposal Due Date	April 21, 2009

1.4 Proposal Evaluation

Proposals will be evaluated based upon the criteria outlined in Section 4 of this document. The contract shall be entered into with the vendor whose proposal is determined in writing to be the most advantageous to the Arkansas Judiciary taking into consideration the evaluation factors set forth in this RFP.

This RFP is being issued solely for the procurement of electronic document management system hardware and software products, and professional services in which no warranty, express or implied, is made to the contractor by the Arkansas Judiciary that any services or products will be purchased during the term of the contract. Any contract awarded pursuant to this RFP shall state that the services will be purchased only on an "as needed" basis. The specific tasks, deliverables, and costs for services purchased under any contract awarded pursuant to the RFP shall be detailed in a written work order signed by both parties.

Any contract awarded shall be:

1. Based upon the response most advantageous to the Arkansas Judiciary, price and

other factors considered.

2. Based upon the demonstrated competence and qualifications for the types of services required and at fair and reasonable prices.
3. Subject to availability of funds.

Funds—approximately $40,000—are available for the purchase of a portion of the requisite hardware, which must be ordered, purchased, and on site by June 30, 2009.

1.5 Proposal Discussions

Discussions may be conducted with responsible offerers who submit proposals determined to be reasonably susceptible to permit a contractual agreement for the purpose of clarification to assure full understanding of, and responsiveness to, the solicitation requirements. Proposers shall be accorded fair treatment with respect to any opportunity for discussion and revision of proposals, and such revisions may be permitted after submissions and before finalization of a contract for the purpose of obtaining best and final offers. In conducting discussions, there shall be no disclosure of any information derived from proposals submitted competing offerers.

SECTION 2
INSTRUCTIONS AND PROCEDURES

2.1 Vendors who wish to submit proposals for the RFP shall complete all necessary documentation as identified in Section 5.

2.2 The specifications included in this package provide adequate information as to whether or not vendors can meet the needs of the Arkansas Judiciary. Significant deviations from the specifications may be grounds for disqualification of the proposal.

2.3 The vendor has sole responsibility for any contracts or agreements made with any subcontractors in relationship to this RFP, and shall disclose all such agreements.

2.4 <u>Preparation of the Proposal</u>

A. Vendors are expected to examine all rules, documents, forms, specifications, standard provisions, and all instructions.

B. Each vendor shall furnish all information required by this RFP. The vendor should refer to Section 5, which contains the proposal submittal checklist, to ensure all required materials have been enclosed. This section also specifies the content and organization of the information to be provided in the response.

C. Time, if stated as a number of days, will be calendar days.

2.5 Explanation to Proposers

Any inquiries related to this RFP are to be directed in writing to the contact person below. Any verbal or written inquiries direct to anyone other than the contact person specified below will not be considered.

2.6 Submission of Proposal

A. Sealed proposals are due on or before April 21, 2009, to Susan Williams, Arkansas Supreme Court Reporter of Decisions, 625 Marshall St., Suite 1400, Little Rock, Arkansas, 72201. Questions may be directed to Susan Williams, susan.willians@arkansas.gov. Proposals must be in the actual possession of the Reporter on or prior to the exact time and date indicated. Late proposals will not be considered under any circumstances.

B. Proposals must be submitted in a sealed envelope with the vendor's name and address clearly indicated on the outside of the package. The vendor must mark on the envelope containing the proposal "PROPOSAL FOR ELECTRONIC DOCUMENT MANAGEMENT SYSTEM/ELECTRONIC PUBLICATION OF OPINIONS."

C. The vendor must submit one original and 3 copies of each proposal.

D. Erasures, interlineations, or other modifications in the proposal must be initialed by a person authorized to sign the proposal and contract.

E. The ROD shall hold all proposals and modifications in a secure place until the due date, after which time the proposals and modifications, if any, will be opened in the presence of at least two State employees, and a register of proposals will be prepared.

2.7 The contract shall be entered into with the responsible vendor whose proposal is determined in writing to be the most advantageous to the Arkansas Judiciary, taking into consideration the evaluation factors set forth in the RFP.

SECTION 3
SPECIFICATIONS

3.1 Purpose and background

A. Purpose

Historically, the task of the of the Reporter of Decisions has been to prepare the opinions and judgments of the Arkansas Supreme Court and Arkansas Court of Appeals for official publication in bound volume format. There has been a significant decrease in demand for the bound volume format due in large part to lack of storage space and greater access to the Internet where opinions may be retrieved from a variety of electronic sources.

During recent years, Internet use has had a major impact on the research methods of attorneys and the practice of law in Arkansas. The headnoted official opinion texts from both appellate courts have been posted on the Arkansas Judiciary Home Page . . . . Judges and attorneys alike have come to rely increasingly on the electronic version of the law reports. *In re Publication of the Arkansas Reports*, 352 Ark. App'x 581, 581-82 (2003).

The Arkansas Supreme Court and Arkansas Court of Appeals now intend to replace the bound volume format with an on-line publication format. The opinions will be accessed via the Arkansas Judiciary Website and will be considered "official," and must be authentic as defined and discussed by the Government Printing Office and the Association of Reporters of Judicial Decisions (see Exhibits 1 & 2). Permanent public access will also be a predominant concern. The EDMS, including imaging, document management, and work flow will be utilized to bring about this objective.

B. Background Information

General

CURRENT ENVIRONMENT

The Arkansas Supreme Court has one Chief Justice and six associate justices elected statewide for eight-year terms. In addition to its appellate jurisdiction, the Court has general superintending control over all courts in the State of Arkansas. The Court of Appeals is composed of 11 judges and one Chief Judge elected from judicial circuits for eight-year terms.

The official published opinions of the Arkansas Supreme Court and Arkansas Court of Appeals are currently published in the bound volumes of *Arkansas Reports/Arkansas Appellate Reports*. Funding for printing and binding is provided by the state legislature.

All signed opinions of the Arkansas Supreme Court are designated for publication. Ark. Sup. Ct. R. 5-2(a). The Arkansas Judiciary Website contains the court's opinions that are designated for publication from 1994 to present, and that are not designated for publication from December 1999 to the present.

The Arkansas Court of Appeals issues a large number of signed opinions each week, but only those opinions that "resolve novel or unusual questions" are released for publication. Ark. Sup. Ct. R. 5-2(c). The Arkansas Judiciary Website currently contains decisions of the Arkansas Court of Appeals that were handed down from 1994 to present and are designated for publication. This website also contains decisions of the Arkansas Court of Appeals that were handed down from January, 2000, to present, but are not designated for publication.

Under the current system, both courts provide the Reporter's office with electronic copies of the opinions on a weekly basis. These files are then converted to portable document format and posted to the Arkansas Judiciary Website; however, those opinions are not the official, final version as found in the *Arkansas Reports/Arkansas Appellate Reports*.

The Arkansas Judiciary's data communications network is a managed TCP/IP, switched Ethernet architecture over fiber hosted by the Arkansas Department of Information Systems (DIS). Internally, it is a switched, Novell based network on 10/100 Ethernet at the desktop via a mix of CAT 5 and CAT 5e cabling that serves approximately 200 Justice Building users. Public users have access to the Arkansas Judiciary Website that is located at and hosted by DIS at http://courts.arkansas.gov/ The new EDMS is also expected to be hosted at DIS with Justice Building access provided through a web client. The implementation of the imaging and workflow system operating software, images, and indexes should not be stored on the mainframe.

The Arkansas Judiciary is currently using a mixture of Windows XP and Windows Vista as the Desktop Operating System.

3.2 STATEMENT OF WORK

A. Summary Statement of Work

The initial scope of the project will include the Reporter of Decisions' office, and will require ten users. This will be subject to change as more users throughout the Justice Building—approximately 110—are phased into the project. At least two people in the ROD will require full access, while the remainder will need only limited access, as well as the ability to search, view, print, and scan. For this initial phase, all of the documents are text and graphics—tables, charts, forms, etc.

B. Detailed Statement of Work

Description of Services and Products Requested*

1. System Overview

The proposed solution must be scalable to the Arkansas Judiciary's current environment and projected growth. File formats, databases and equipment requirements should be nonproprietary. Provide an overview description of the products you recommend to address the ROD's imaging, document management, and workflow needs. Describe the proposed system's scalability and its compatibility with the overall environment of the Arkansas Judiciary.

2. Information Input

The system should offer the ROD at least three different ways to bring documents into the document imaging system: scanning (books and documents), electronic conversion into images, and importation of documents in their native file format.

The system should work with most common scanning drivers and support scanner features such as multiple image resolutions, paper sizes, duplex scanning and automatic document feeders. It should also be able to display images as they are scanned so that the operator can visually verify image acceptability. The system should allow for both batches of documents and individual document scanning. Describe the image enhancement capabilities of the system, which should include at a minimum deskew, despeckle, blank page detection and rotation features. The system must allow individual pages to be rescanned or added to an existing document when additional pages need to be added. The system must allow the capability to reorganize pages within a document. An automatic naming document naming ability is important, allowing any or all of the following information to be added: user name, date, time or a sequential document number.

Storage of electronic documents in an archival, nonproprietary format is necessary. The system must easily create images of electronic documents and import them into the system.

Storage of electronic documents in their native file format is necessary.

3. Indexing and Retrieval

The system should include Optical Character Recognition (OCR) software that will generate text files for documents that are scanned or electronically converted into images; this text file will be used for full-text indexing and searches. Full-text retrieval should support Boolean logic, "fuzzy" logic, and proximity searches. The system should support multiple keyword index templates, with each template having multiple fields. These indexes should support searchable character, date, and integer fields, with options for automating their information entry. The system should support a folder/file structure similar to that of Windows Explorer, with multiple levels of folders available. Index templates and folder structure should be user-definable.

The system should give users multiple options for searching and retrieving documents. The ROD plans to recreate its existing paper folder/file structure in electronic form on the new system. Users should be able to retrieve documents visually based on their folder location, by full-text keywords or by a combination of methods.

3. Viewing

The system should have an easy to use graphical user interface and support various viewing options, including zoom, rotate image, increase/decrease brightness, etc. The software should also allow users to select whether to view image, OCR text, index information or thumbnails. Users should be able to concurrently view multiple images of various types while performing data entry functions in another window. Describe viewer capabilities provided by the software to support the viewing of imaged documents.

The system should support annotations such as highlighting, sticky notes, digital watermarks/electronic "stamps" [to be used to authenticate documents in accordance with the definitions and requirements set out in Exhibits 1 & 2] and redaction (blackout and whiteout). Please describe the annotations supported by the proposed system.

4. Information Output

All imaged documents should be printable with or without annotations. Each document must be printable in its entirety, as well as for a single page or selected range of pages. Multiple users should be able to print the same document concurrently. Users should be able to fax or e-mail imaged documents either internally or externally using [MAPI-compliant] e-mail software.

Please describe the printer capabilities supported by the software, including color, duplex and maximum document size. Describe the ability of the software to fax and e-mail documents. Describe the ability of the software to support data mining methods and processes, including search capabilities, query support, and standard statistical and management reporting.

5. Security and Audit

The proposed system must allow the the system administrator the ability to protect confidential documents at the folder, document, word and annotation levels for both internal and Internet access. The system must allow for the creation of user and group profiles that allow access to the document management system and govern which records can be accessed and what actions can be performed on the records being accessed or added to the system.

Security should be granular and able to be set by user, group, folder, document and system command or function.

Describe the audit functions and capabilities in support of a paperless audit trail, including change and event log reporting, productivity reporting functions and capabilities, and imaging and workflow/document software.

6. Workflow/Document Management

Workflow/Document Management will be implemented in stages as additional users are phased in throughout the Justice Building. The proposed system should allow support by department [judges and staff/clerk's office etc.] or document type, inputs from multiple sources, intelligent routing, workload management, e-mail notification and parallel work processing. The system should alert specific users of specific events within the system, and be easily modified by system administrators.

Describe the capabilities of the workflow software, including platforms supported, process design tools, rules engine and reporting. Describe the assignment of workflow processes, work roles and specific users and how the system identifies which tasks users belonging to multiple groups should perform. Describe how the system assures that workflow related to a specific item has been completed and how the system can be extended to interact with other software.

7. Hardware

Please describe the recommended server configuration for the system. Include warranty, network protocol, any additional software required, and how the proposed system will integrate with the ROD/Arkansas Judiciary's existing environment. Describe the recommended optical storage medium, the storage capacity of this medium, and retrieval times associates with it. Quotes will need to allow for whatever hardware is necessary to store data for the initial phase of the project.

9. Web Interface

The proposed solution should have a web interface allowing authorized users to search and view documents from any computer with Internet access and a modern web browser. The system administrator/website coordinator should be able to specify which documents are publicly accessible via the web and what document functions are available to be performed by web users.

9. Support, Training, and Implementation

Please outline recommendations and plans for assisting the ROD and IT staff with pre- and post-implementation support. This includes on-site training, telephone support, and proposed response times

C. Costs

The vendor must provide specific costs for the ROD to implement each phase of the EDMS, which shall include separate headings for the following:

1. **Hardware procurement**
2. **Hardware maintenance**
3. **Operating system procurement**
4. **Operating system maintenance**
5. **EDMS software procurement**
6. **EDMS software maintenance**
7. **Technical training and support—pre-and post implementation.**
8. **Annual licensing/warranty/upgrade costs**

SECTION 4
PROPOSAL EVALUATION CRITERIA

Proposals will be evaluated based upon the following criteria. The evaluation criteria are listed in order of relative importance.

EVALUATION CRITERIA RELATIVE IMPORTANCE

A. Cost 35%

The cost of the solution, including individual licenses, hourly costs for services, on-going support and maintenance costs.

B. Qualifications and Relevant Experience 35%

1. An evaluation of vendor qualifications and expertise in the area of electronic document management systems and the standardized product sets based on summaries of and contact information for similar projects conducted by the proposed consultant(s).
2. An evaluation of vendor qualifications and knowledge of court environment based summaries and contact information for technology-related projects performed by the proposed consultant(s) in court environments.

C. Methodology Proposed 30%

1. Completeness and responsiveness to the services and deliverables specified in this RFP.
2. Structured phasing of work.
3. Evidence of project understanding and scope.

SECTION 5
PROPOSAL SUBMITTAL DOCUMENTS

Proposal Submittal Checklist

The following materials must be submitted as part of a vendor response:

5.1 Proposal Submittal Letter (see page 12)

5.2 Three references from organizations with similar structures and requirements

5.3 Vendor Profile (see page 13)

PROPOSAL SUBMITTAL LETTER

(Use as page 1 of proposal)

Susan Williams
Reporter of Decisions
Arkansas Supreme Court
625 Marshall Street, Suite 1400
Little Rock, Arkansas 72201

Dear ________________:

In response to your Request for Proposal (RFP) please accept the following:

In submitting this proposal, I hereby certify:

1. that the RFP has been read and understood;
2. That the materials requested by the RFP are enclosed;
3. That all information provided is true, accurate, and complete to the best of my knowledge;
4. That this proposal is submitted by, or on behalf of, the party that will be legally responsible for service delivery should a contract be awarded.

____ ______________________
Signature of Authorized Official Date

Name of Signatory: ____

Company: ____

Title: ____________________________ Phone: _____________________

Address: ______________________________________

____

____

Federal Employer ID# or SSN#:_________________________________

VENDOR PROFILE

Please provide the following information about your company:

1. What is the physical mailing address and fax number of your company's main office?.

2. Who in your company will be our primary point of contact during the proposal evaluation process? (Please provide name, title, direct phone number, e-mail address, fax number, and mailing address.)

3. Who in your company is authorized to negotiate a contract with us? (Please provide name, title, direct phone number, fax number, and mailing address.)

4. Provide a brief history of your company.

5. Indicate the total number of employees in your company and their distribution by function.

Exhibit 1

GPO
U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED

Authentication

U.S. Government Printing Office
Office of Information Dissemination
Program Development Service

Washington, D.C.

October 13, 2005

Contents

I. PREFACE

In accordance with GPO's strategic vision, GPO has identified a need to develop policies and create systems that address the authentication and certification of electronic Government publications. As outlined in the Future Digital System (FDsys) Concept of Operations document, GPO will create an authentication system to verify the authenticity of digital content within the FDsys, and certify this to users accessing the content. In the near term, GPO is currently implementing a Public Key Infrastructure (PKI) initiative to ensure the authenticity of its electronically disseminated content on *GPO Access*.

It is important to note that this white paper is now considered to be complete. However, GPO will continue to plan and implement the authentication initiatives that meet the needs of the user community. GPO will continue to provide updates and solicit public comments on this issue through other channels, including Federal depository library conferences and voice of user activities conducted in conjunction with the implementation of GPO's Future Digital System.

II. OVERVIEW

GPO recognizes that as more Government publications become available electronically, confidentiality, data integrity, and non-repudiation become more critical. The primary objective of GPO's authentication initiative is to assure users that the information made available by GPO is official and authentic and that trust relationships exist between all participants in electronic transactions. GPO's authentication initiatives will allow users to determine that the files are unchanged since GPO authenticated them, help establish a clear chain of custody for electronic documents, and provide security for and safeguard Federal Government publications that fall within scope of the National Collection of U.S. Government Publications.

A. Definitions

The following definitions will be applied to the terms below throughout this paper.

- Authentic Content – Describes content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator.
- Authentication – Validation of a user, a computer, or some digital object to ensure that it is what it claims to be. In the specific context of the Future Digital System, the assurance that an object is as the author or issuer intended it.
- Authenticity – A digital publication's identity, source, ownership and/or other attributes are verified. Authentication also connotes that any change to the publication may be identified and tracked.
- Certification – Proof of verification or authority. Process associated with ensuring that a digital object is authentically the content issued by the author or issuer.

- Certificate – Mark of veracity that conveys certification information to users and is in some way joined to the object itself.
- Integrity Mark – Conveys authentication information to users. The integrity mark will include certification information and may include an emblem. Integrity marks are used to convey certification by providing verification of content as authentic and/or official.
- Official Content – Content that is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications.
- Government publication – A work of the United States Government, regardless of form or format, which is created or compiled in whole or in part at Government expense, or as required by law, except that which is required for official use only, is for strictly operational or administrative purposes having no public interest or educational value, or is classified for reasons of national security.
- Publication – (N) Content approved by its Content Originator for release to an audience. See also Government publication.

III. SCOPE

Policies, procedures, and guidelines put forth by GPO on authentication will apply to all publications that are deemed to be within the scope of the FDLP, with a particular emphasis placed on publications that are disseminated electronically. This document will not address authentication issues related to tangible publications or documents that have not been approved by Federal publishing agencies for dissemination to the general public.

IV. KEY ASSUMPTIONS

1. GPO's Authentication system will provide the capability for GPO to certify content as authentic and official.
2. GPO's Authentication system will provide the capability to verify and validate that deposited, harvested, and converted content are authentic and official.
3. GPO will convey authentication information to users through the use of an integrity mark.
4. Chain of custody information should be included in the certification information when available.
5. GPO's Authentication system will provide date and time verification for certified content.
6. Documents residing on *GPO Access* are official[1], and retrospective authentication will be used to add integrity marks that reinforce this status.

[1] All *GPO Access* documents are official in the sense that they are published by the Federal Government, at Government expense, or as required by law. GPO recognizes that there are connotations of the term "Official", especially in the legal community, that differ from this definition. GPO is currently working on language to address this discrepancy.

7. GPO's Authentication system will re-authenticate the version of content that has been authenticated at earlier stages in the publishing process by GPO or Content Originators. For example, if there is a digital signature attached to a file when it comes into GPO from a publishing agency, GPO will be able to record that information and carry it forward in the provenance or in the chain of custody and provide that information to user.
8. When authentication information is already available from the Content Originators (e.g., publishing agencies), GPO should retain and display that information.
9. GPO's Authentication system will provide the capability for GPO to change the authentication status of content.
10. GPO's Authentication system should have the ability to certify a related or continuous piece of content in context (e.g. level of granularity).

V. CURRENT STATE

GPO is currently implementing a PKI initiative to authenticate the files available through *GPO Access*. GPO will use digital signature technology to certify documents as official and authentic. When fully implemented, GPO will be able to ensure confidentiality, authenticity, integrity, and non-repudiation of electronic transactions using digital signatures.

VI. KEY ISSUES

A. Level of Authentication

The provenance and fixity of an electronic document is directly related to its level of authentication. GPO will inform users about a publication's integrity and chain of custody through the designation of at least 2 different levels of authentication, "authentic" and "official." GPO defines "authentic" as content that is verified by GPO to be complete and unaltered when compared to the version received by GPO. "Official" content is content that is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications. There may be instances, however, where GPO will harvest information that cannot be confirmed as official by the content originating agency. An example is a publication harvested from the Internet Archive Wayback Machine. This content will be considered authentic but not official by GPO.

B. Content Format

It will be necessary for GPO to authenticate and certify all content formats disseminated by GPO. Content formats may include but not be limited to PDF, ASCII text, video, audio, graphic, and multimedia. GPO must develop appropriate authentication and certification methods for all content formats available from GPO.

C. Integrity Mark

The process of certification will produce an integrity mark that will include certification information and may include an emblem. Integrity marks will allow users to determine if files have been changed since GPO authenticated them, and help establish a clear chain of custody for electronic documents. Emblems may be presented to users in various ways, such as a logo used in conjunction with a digital signature. GPO will also investigate emerging technologies related to the certification and authentication of non-digital content formats (e.g., digital watermarking of GPO publications downloaded and printed by users).

1. Emblem

GPO may provide an emblem to notify users of the authentication status of a publication in accordance with the required approval, when feasible, of the content originator. Different content formats (e.g., audio, video, etc.) will require the use of emblems that are appropriate for each format. Users may be required to initiate additional procedures to access emblems associated with different content formats.

Look and Feel

When an emblem is visibly displayed, it should contain the official GPO authentication seal and/or official seal for the publishing agency.

Placement

When an emblem is visibly displayed, it should be placed in the same location on every document. This location should not interfere with the contents of the publication (e.g., the visible emblem should not obstruct the title of the document). The upper left hand corner is a suggested placement for the visible emblem, but additional analysis will need to be performed to ensure that this will work for all electronic publications available from GPO.

2. Certification Information

All integrity marks will include certification information. It is recommended that the following information be available in the certification information. This information may also be contained in a digital certificate.

- Certifying organization
- Date of the signature/certification
- Digital time stamp
- Public key value
- Hash algorithm used
- Reason for signing
- Location
- Contact information
- Name of entity that certified the publication
- Level of authentication
- Expiration date of signature / certification

- Notification of changes occurring to the document

D. Granularity

The level of granularity to which a publication should be certified is a planning issue that must be addressed in conjunction with the implementation of the Future Digital System. Presently, a technology gap exists in that GPO currently only has the technology to authenticate at the entire document level, meaning that the content as a whole will be certified in its complete state.

GPO's future authentication plans must include a means by which sections or small pieces of a publication (i.e. document) are authenticated and digitally certified. GPO's Future Digital Authentication system should have the ability to certify a related or continuous piece of content in context (i.e. level of granularity) as defined by GPO and based on user needs.

In addition, integrity marks and certificates should be available at all levels of granularity delivered to users. For example, if a user is able to retrieve a section of a CFR title, the section should be certified. The entire part of the same title should also contain an integrity mark and certificate.

The policies for granularity will need to be set based on realistic expectations of technology advancements and evolving requirements of users. To this end, significant data will need to be collected by GPO in order to determine what levels of granularity users require for each content format. Granularity policies developed by GPO must be adaptable and flexible such that they may be changed in response to changes in user requirements or changes in methods/formats of dissemination preferred by originating agencies.

E. Chain of Responsibility

GPO will certify publications as "official" on behalf of Congress, Federal agencies, and other Federal Government organizations. Publications will be certified as "official" if the content originators (e.g., Congress, Federal agencies, commissions, committees, courts, etc.) have given GPO the authority to certify publications, or if the content has been contributed by or harvested from an official source in accordance with accepted program specifications. In the case of most documents already available on *GPO Access*, Federal organizations have given GPO official content to disseminate via the FDLP, and GPO is able to verify the chain of responsibility in order to certify documents as "official."

F. Retrospective Authentication

It will be necessary to authenticate all files on *GPO Access*. As GPO moves forward with its retrospective authentication process, there may be occasions where some files on *GPO Access* will contain integrity marks and certificates, but some will not. In this case, it is important to note that all files currently residing on *GPO Access* are official and the authentication process will reinforce the status of these documents.

G. Maintenance

Through out the lifecycle of an authenticated publication, it will become necessary to periodically "re-authenticate" the publication.

VII. CONCLUSION

Ensuring customers that the electronic information made available through GPO is official and authentic is of paramount importance for our future. There is a need for information that is reliable because it is from a trusted source, and a need to ensure the protection of data against unauthorized modification or substitution of information.

The steps that have been taken to stand-up a PKI and the associated digital signature process used in accordance with the policies and infrastructure of this system will enable GPO to assure customers that electronic files are unchanged since being authenticated by GPO. GPO's authentication processes will allow customers to verify that a document originally disseminated by GPO is exactly the same as the document downloaded by the customer.

Equally important, the steps that GPO has already taken as part of its authentication effort map directly to requirements that are under development for the Future Digital System. Additional issues that are not currently being addressed, such as how to authenticate information at granular levels, are being addressed as new requirements based upon customer feedback.

VIII. RESOURCES

Public Key Infrastructure (PKI) Business Plan, October 28, 2003.

GPO's Future Digital System Concept of Operations Version 2.0, May 2005, http://www.gpo.gov/projects/pdfs/FDsys_ConOps_v2.0.pdf.

Internet Archive Wayback Machine, May 2005, http://www.archive.org/web/web.php.

IX. ACRONYMS USED IN THIS PAPER

FDsys – Future Digital System

PKI – Public Key Infrastructure

X. SUMMARY OF PUBLIC COMMENTS

GPO released this White Paper to the public on June 23, 2005, requesting that comments be submitted by August 8, 2005. In response to requests, GPO extended the deadline for comments to September 16, 2005, and made samples of authenticated documents available for review in conjunction with the White Paper. The following is a summary of the comments.

Comments

GPO was commended on its ongoing efforts to develop policies related to the management of electronic publications. The consensus was that the paper does a thorough job of identifying many of the key issues. There were several specific areas of concern identified, and they are listed below:

1) The centrality and significance of authenticating information at granular levels
2) The methods for authenticating web pages, which lack the fixity of PDF documents.

These issues are fundamental to the definition of what a document is, and whether individual documents are the appropriate or the only unit measure for authentication. Further exploration and clarification of these issues are needed to assure that the concept of a "document" is not the sole factor in determining the authenticity of an electronic source.

GPO received comments noting that some resources available on GPO Access (e.g., Supreme Court Decisions, 1937-1975) are not official. Moreover, it was noted that 'official' has a more specific meaning in the rules of legal citation than in GPO's definition. An official version is the one designated as such by the issuing body and to which a citation must be made. Furthermore Rule 18 in the just released 18th edition of The Bluebook: A Uniform System of Citation, "requires the use and citation of traditional printed sources unless (1) the information cited is unavailable in a traditional printed source; or (2) a copy of the source cannot be located because it is so obscure that it is practically unavailable." Thus an electronic version could be cited to only when there is no paper version of a document or that version cannot be found. Commenting organizations stated that GPO also needs to expand the definition of 'official' to include some statement that even if the content has been certified to be the same as the printed version, it may not be 'official' in the legal sense.

GPO Response

GPO recognizes the centrality and significance of authenticating information in multiple file formats and levels of granularity. These capabilities are currently requirements of the authentication portion of the Future Digital System and GPO continues to work toward implementation of these capabilities.

All *GPO Access* documents are official U.S. Government information in the sense that they are published by the Federal Government, at Government expense, or as required by law. GPO recognizes that there are connotations of the term "Official", especially in the legal community, that differ from the definition of official as stated in this White Paper. For example, the Administrative Committee of the Federal Register has stated that both the online and print versions of the Code of Federal Regulations and Federal Register are "Official," while the Supreme Court and the Law Revision Counsel of the U.S. House of Representatives have stated that the online versions of Supreme Court Slip Opinions and the U.S. Code, respectively, are not "Official" for purposes of legal citation. Nevertheless, all of these online titles are official Federal Government information in the sense that term is used in this document. GPO is currently working on language to address this discrepancy.

Exhibit 2

Association of Reporters of Judicial Decisions

WILMA M. GRANT, *President*
Publishing Manager/Ofc. of Data Sys.
Supreme Court of the United States
Rm. G-20 - One 1st Street, NE
Washington, DC 20543
202-479-3455 Fax: 202-479-2965
wgrant@supremecourt.gov

KEVIN J. LOFTUS, *Vice-President*
Reporter of Decisions
Supreme Court of Connecticut
231 Capitol Avenue
Hartford, CT 06106
860-757-2252 Fax: 860-757-2213
kevinloftus@connapp.state.ct.us

CLAUDE MARQUIS, *Secretary*
Chief Law Editor - Law Branch
Supreme Court of Canada
301 Wellington Street
Ottawa, (Ont.) K1A 0J1
613-996-2394 Fax: 613-947-5033
marquisc@ssc-csc.gc.ca

TRUMAN S. FULLER, *Treasurer*
Reporter of Decisions
Supreme Court of Washington
Temple of Justice, P.O. Box 40929
Olympia, WA 98504-0929
360-357-2090 Fax: 360-357-2099
tim.fuller@courts.wa.gov

STATEMENT OF PRINCIPLES: "OFFICIAL" ON-LINE DOCUMENTS

Issued: February, 2007
Revised: May, 2008

The Association of Reporters of Judicial Decisions (ARJD) is an international organization of public servants whose primary responsibility is to prepare the opinions and judgments of appellate and other courts for official publication. In many courts, the Reporter of Decisions is also the primary archivist and repository of official opinions. As an organization dedicated to the dissemination, publication, and accurate reporting of court decisions, the ARJD recognizes that serious issues have arisen regarding the preservation, authenticity, and certification of official government documents, especially with regard to on-line and electronic versions of those documents. The following policy statement represents the position of the ARJD and its members on those issues. By publicizing its views, the ARJD hopes to alert its public-sector colleagues to the reality that the on-line publication of unauthenticated and impermanent "official" documents in an attempt to save publication costs may unwittingly result in the adulteration or loss of valuable and irreplaceable primary government source materials. Because court opinions frequently cite and rely on such materials, their preservation and authenticity are of paramount concern to the ARJD's members.

1. A government document should not be considered "official" unless it is authorized by law or is designated "official" by the governmental entity that issued it. Court reports printed pursuant to statutory or judicial authorization are traditional, prototypical examples of "official" government documents. See, *e.g.*, 28 U. S. C. §411 (authorizing the printing and binding of the opinions of the Supreme Court of the United States in the official United States Reports). Absent statutory authorization, each individual state or federal court is the arbiter of what constitutes its "official" reports.

2. There should be only one "official" version of a document in existence at any one time. Any given document has certain content, and the purpose of designating one version of that document as "official" is to denote, for legal and all other purposes, exactly what that content is. For example, if the document in question is a United States Supreme Court opinion and the bound volume of the U. S. Reports is designated as the "official" document, what is posted on the Court's Website is an electronic copy of the "official" document, but it is not itself "official." Discrepancies between print and electronic versions of a particular government document may be quickly and easily resolved if one, but only one, of those versions has been designated "official."

3. Print publication, because of its reliability, is the preferred medium for government documents at present. For example, official court reports are relied upon as authoritative and definitive guidance in conducting legal dealings and affairs because of the reports' undoubted and demonstrable authenticity and their existence in a permanent, published form. Similarly, on-line government documents should not be designated "official" unless they are (1) authenticated by encryption, digital signature, or some

other computerized process to safeguard them from illegal tampering and (2) permanent in that they are impervious to corruption by natural disaster, technological obsolescence, and similar factors and their digitized form can be readily translated into each successive electronic medium used to publish them. So long as no computerized process guarantees such permanence, a governmental entity should not designate a non-print-published, electronic document "official" unless there is a statute or administrative regulation in the particular jurisdiction requiring the authentication and perpetuation of "official" online documents or the issuing governmental entity undertakes to make whatever conversions are necessary in the future in order to perpetuate the document in an accessible, accurate, "official" form.

4. If, notwithstanding the imperative that there be but one official version of a document, a governmental entity chooses to designate multiple co-existing versions (print and/or electronic) as "official," mechanisms must be provided to ensure that each of those official versions meets the foregoing authentication and permanence criteria. With respect to official electronic documents, this requires that appropriate encryption techniques be employed and that the digital formats used to store and process the documents take into account the evolving hardware and software utilized to preserve access to those documents.

5. An on-line government document, even one designated "official," cannot be considered authoritative if it does not satisfy the foregoing authentication criterion. An on-line government document, particularly one designated "official," should never be the sole published version of the document if it does not satisfy the foregoing permanence criterion.

6. So long as only the print version of an official document meets the foregoing authentication and permanence criteria, the print version (and any printed errata thereto) should control and be considered authoritative whenever there is a discrepancy between it and an on-line version of the same document that has also been designated "official." In such an instance, the issuing governmental unit should post a disclaimer with the on-line version establishing the print version's ascendancy in cases of conflict.